

A Two-Decade Retrospective Analysis of a University's Vulnerability to Attacks Exploiting Reused Passwords

Alexandra Nisenoff, Maximilian Golla, Miranda Wei, Juliette Hainline, Hayley Szymanek, Annika Braun, Annika Hildebrandt, Blair Christensen, David Langenberg, Blase Ur



THE UNIVERSITY OF
CHICAGO



Carnegie
Mellon
University



W
UNIVERSITY of
WASHINGTON

People Reuse Passwords

LinkedIn

princess123

Gmail

NETFLIX

Princ3ss123!

CHASE



PayPa

Letmein!



slack

princess99



querty1999



THE UNIVERSITY OF CHICAGO

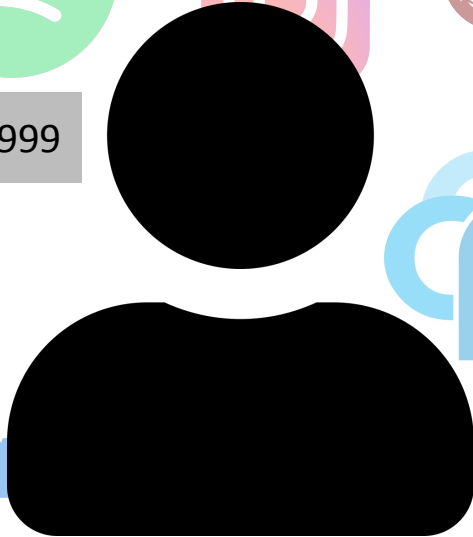
princess123



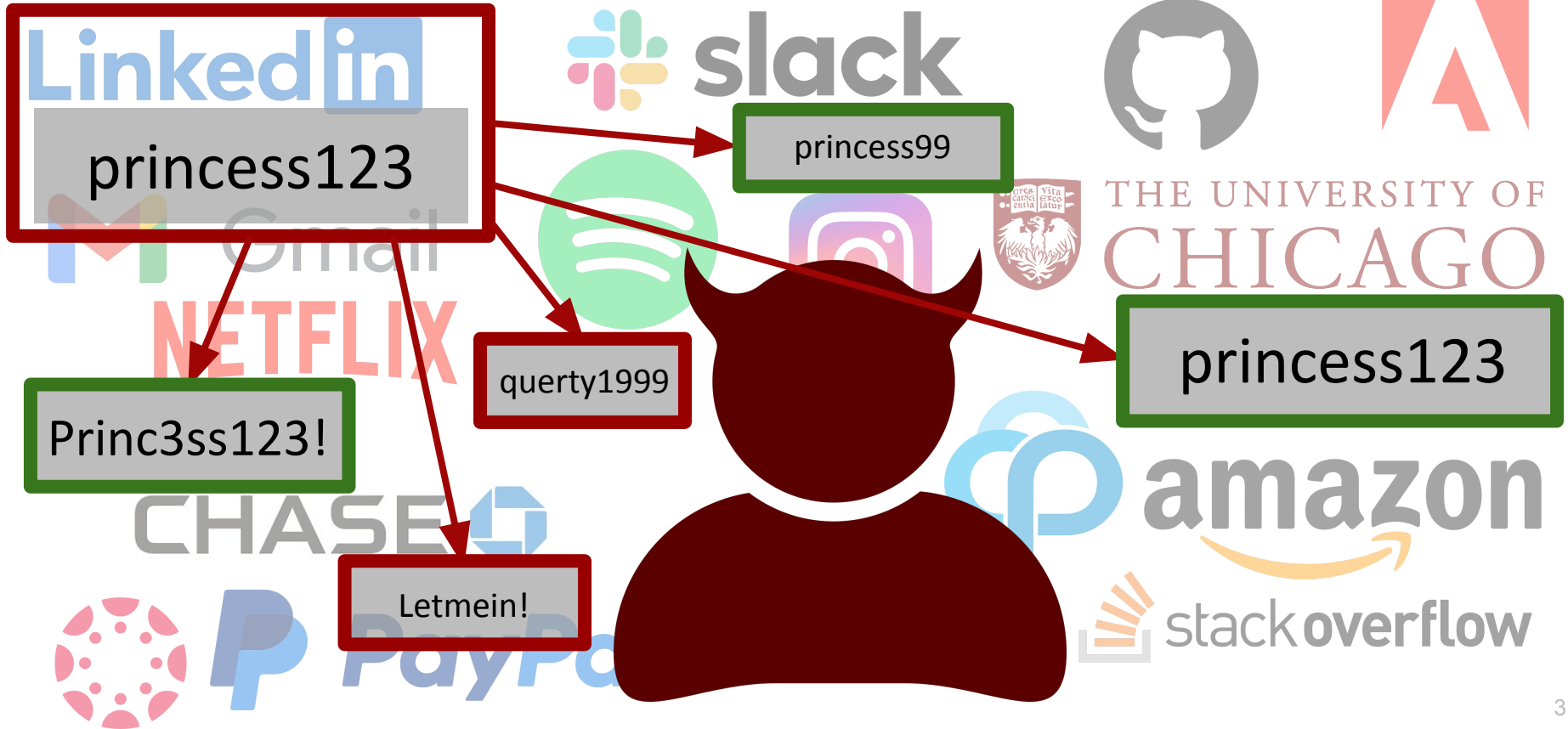
amazon



stack overflow



People Reuse Passwords & Attackers Know



UChicago Password History Database

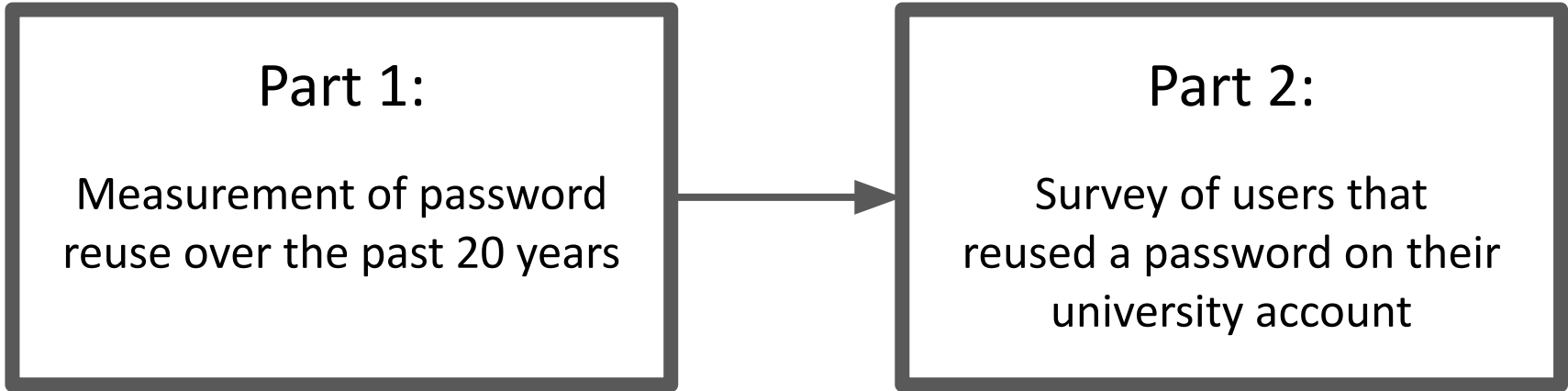
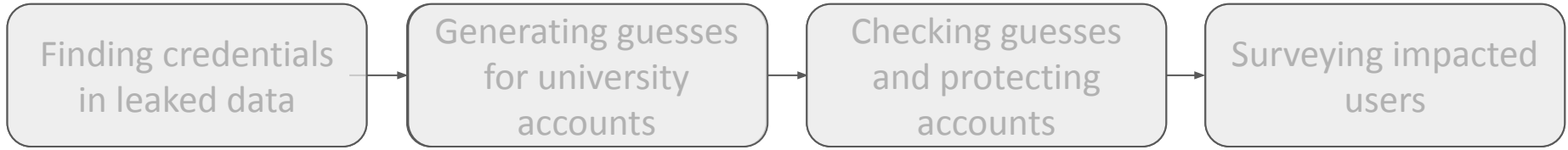
Create Password or Passphrase

You have already used this password before. Please choose a different one.

UChicago Password History Database

Username	Hash of Password	Created	Changed	
weimf	hash(i<3cats1234)	Sep 17, 2016	Jul 1, 2019	...
weimf	hash(i<3cats2019!)	Jul 1, 2019	present	...
hszym	hash(p@nc@kes99)	Aug 15, 2018	present	...
julietteh	hash(Tiwchnt89)	Nov 10, 2017	Aug 23, 2019	...
...

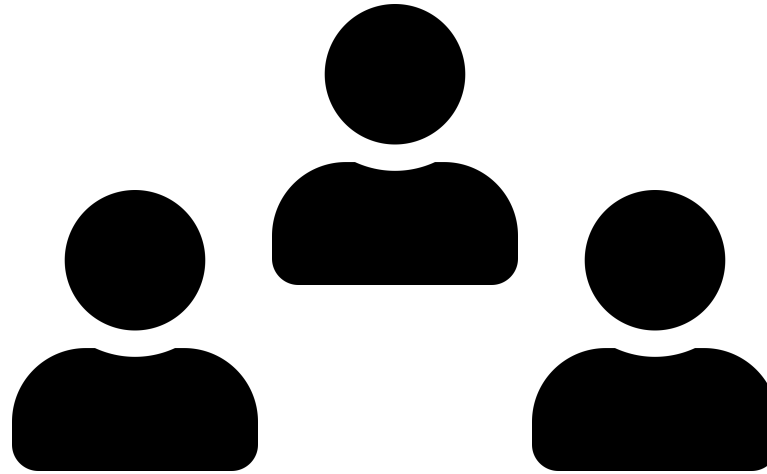


Finding credentials
in leaked data

Generating guesses
for university
accounts

Checking guesses
and protecting
accounts

Surveying impacted
users



227,976 Usernames

Finding credentials
in leaked data

Generating guesses
for university
accounts

Checking guesses
and protecting
accounts

Surveying impacted
users

Sources of Credentials

- 450 individual service breaches
 - LinkedIn, Chegg, etc.

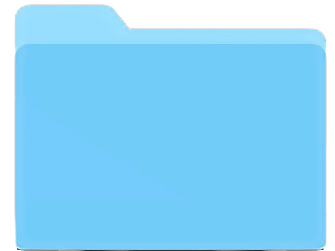








- 12 large breach compilations
 - Collection #1, Anti Public Combo List, etc.



Finding credentials
in leaked data

Generating guesses
for university
accounts

Checking guesses
and protecting
accounts

Surveying impacted
users

username: **nisenoff**



nisenoff@uchicago.edu



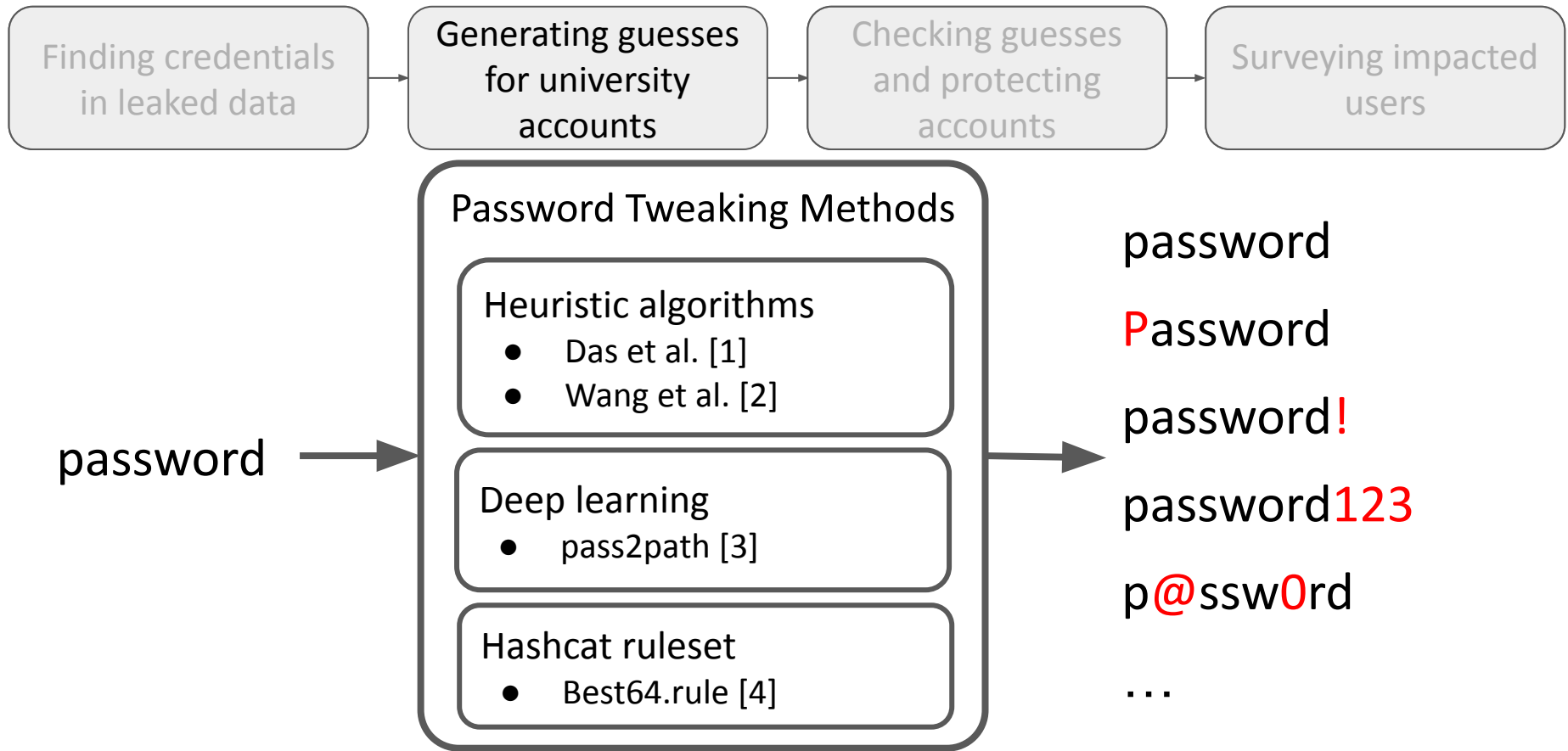
nisenoff@cmu.edu



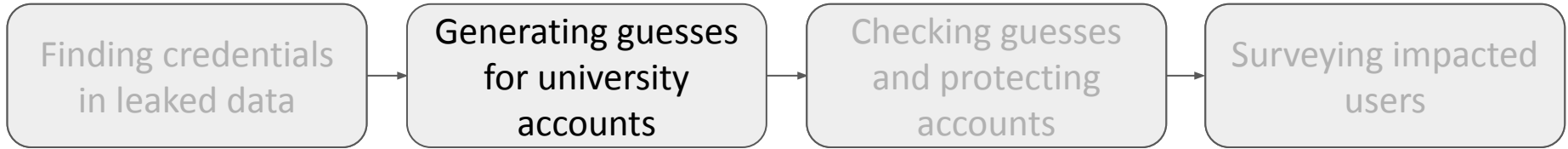
nisenoff



nisenoff99@gmail.com



[1] A. Das, J. Bonneau, M. Caesar, N. Borisov, and X. Wang. The Tangled Web of Password Reuse. In *Symposium on Network and Distributed System Security*, NDSS, 2014.
 [2] C. Wang, S. Jan, H. Hu, D. Bossart, and G. Wang. The Next Domino to Fall: Empirical Analysis of User Passwords across Online Services. CODASPY, 2018.
 [3] B. Pal, T. Daniel, R. Chatterjee, and T. Ristenpart. Beyond Credential Stuffing: Password Similarity Models using Neural Networks. IEEE SP, 2019.
 [4] J. Steube (“atom”) and Community. Official Best64 Challenge Thread, 2012. <https://hashcat.net/forum/thread-1002-post-5284.html#pid5284>



“Common” Password Guesses

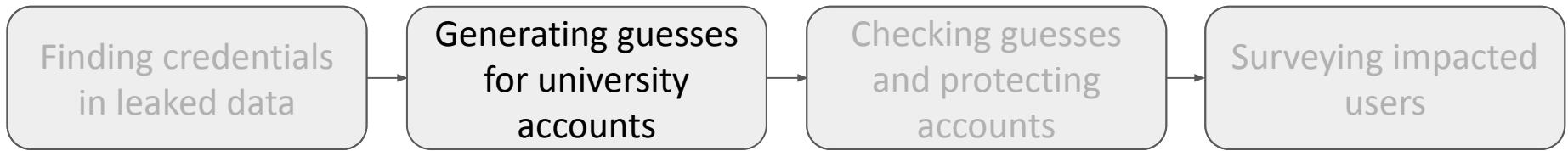


THE UNIVERSITY OF
CHICAGO

password1 → password1

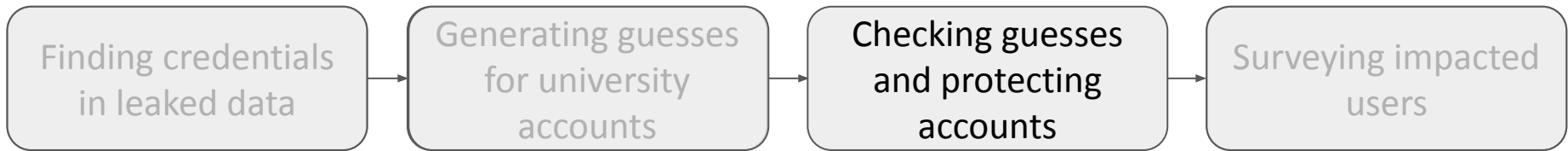
LinkedIn1 → UChicago1

P@ssw0rd1234 → P@ssw0rd1234



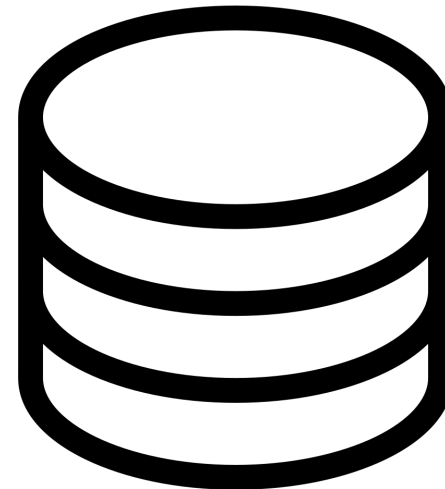
Historical Password Policies

	Time Period	Length	Character Classes
Password	2015 - Present	12 - 19	3+
	2010 - 2015	8 - 16	3+
	Prior to 2010	8 - 16	2+
Passphrase	2016 - Present	18 - 32	1+
	2014 - 2016	18 - 50	1+



Username	Password	...
nisenoff	letmein123	...
blase	qwerty123	...
mgolla	Monkey<3	...
...

Credential Guesses



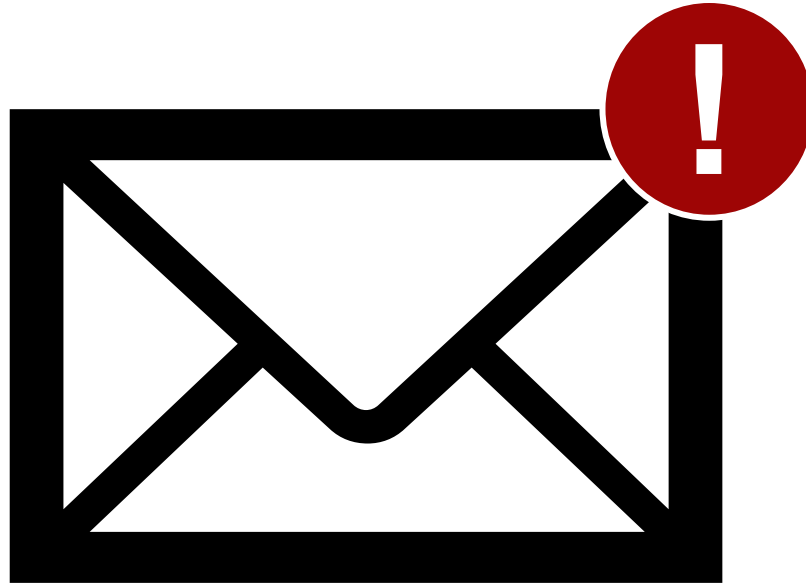
UChicago Password History Database

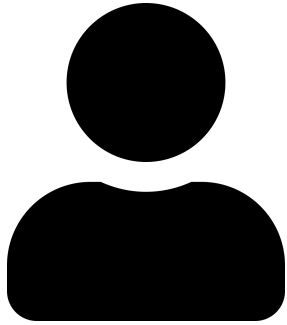
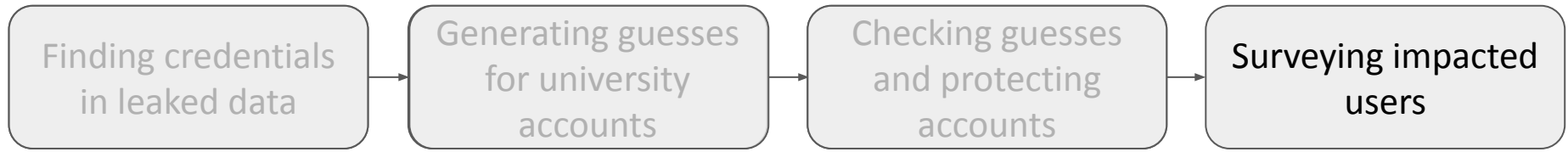
Finding credentials
in leaked data

Generating guesses
for university
accounts

Checking guesses
and protecting
accounts

Surveying impacted
users





40 Participants

Surveys were customized to show participants the sources of data used to guess their password

Ethical Considerations

- Approved by IRB
- Study design informed by discussions with
 - a. IT Leadership (including the CIO)
 - b. Provost's office
 - c. University's communications team
 - d. University's general counsel
 - e. Alumni association
- Minimizing access to password history database
- Password resets

12,247 correct guesses
based on password reuse

We Guessed at Least One Password For:

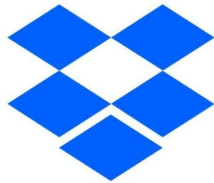
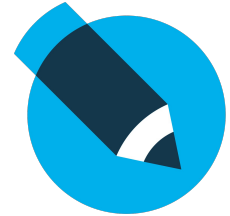
- **4.5%** of all users
- **6.5%** of users that we made a guess for
- **32.0%** of users with a uchicago.edu email in a data breach

We guessed the current password for
3,618 accounts

Correct Guesses Came From 71 Individual Service Breaches
and All 12 Breach Compilations

LinkedIn

Chegg



myspace

COMCAST

neopets®

Forbes

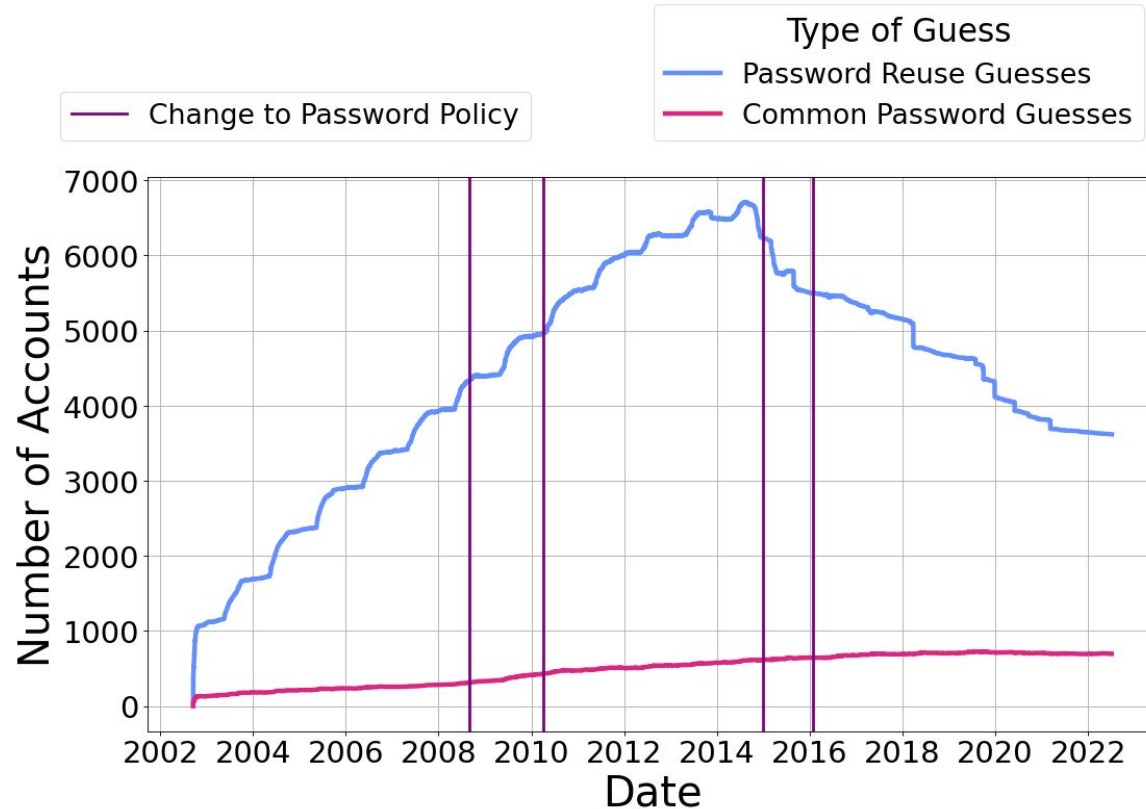
last.fm

wattpad



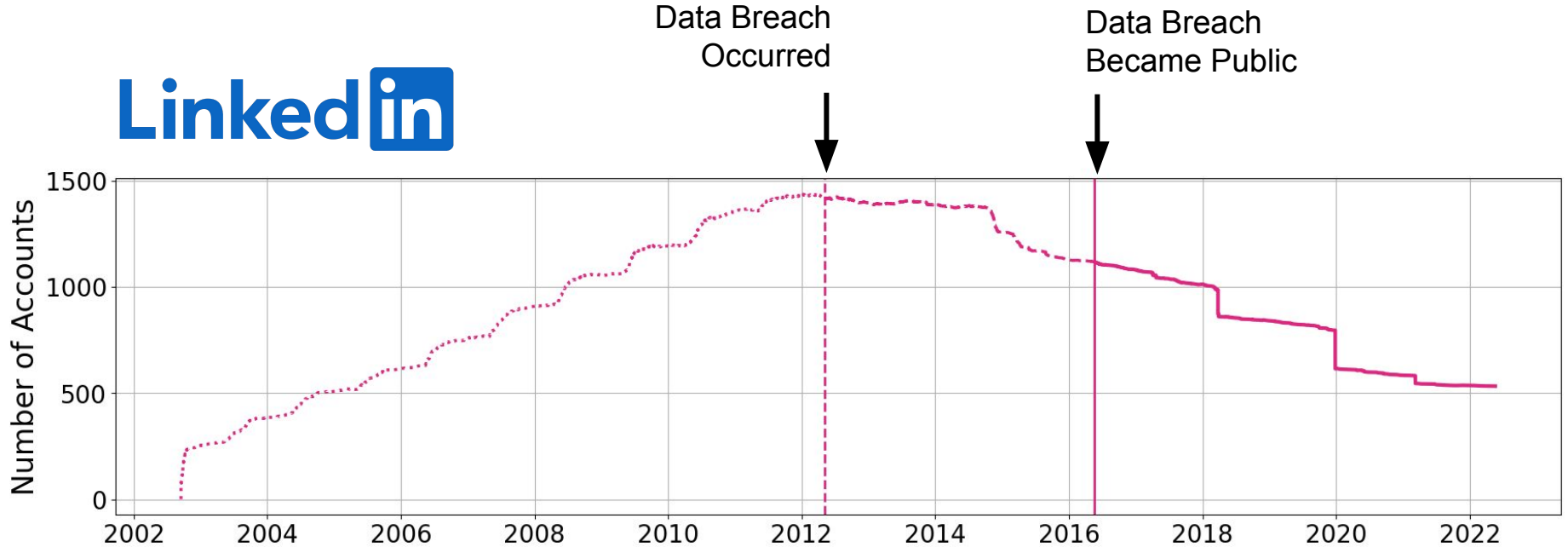
yahoo!

The Number of Accounts That Use Reused Passwords Changes Over Time



Reused Passwords Can Stay Valid for a Long Time

... Even Relative to When Data Breaches Happened



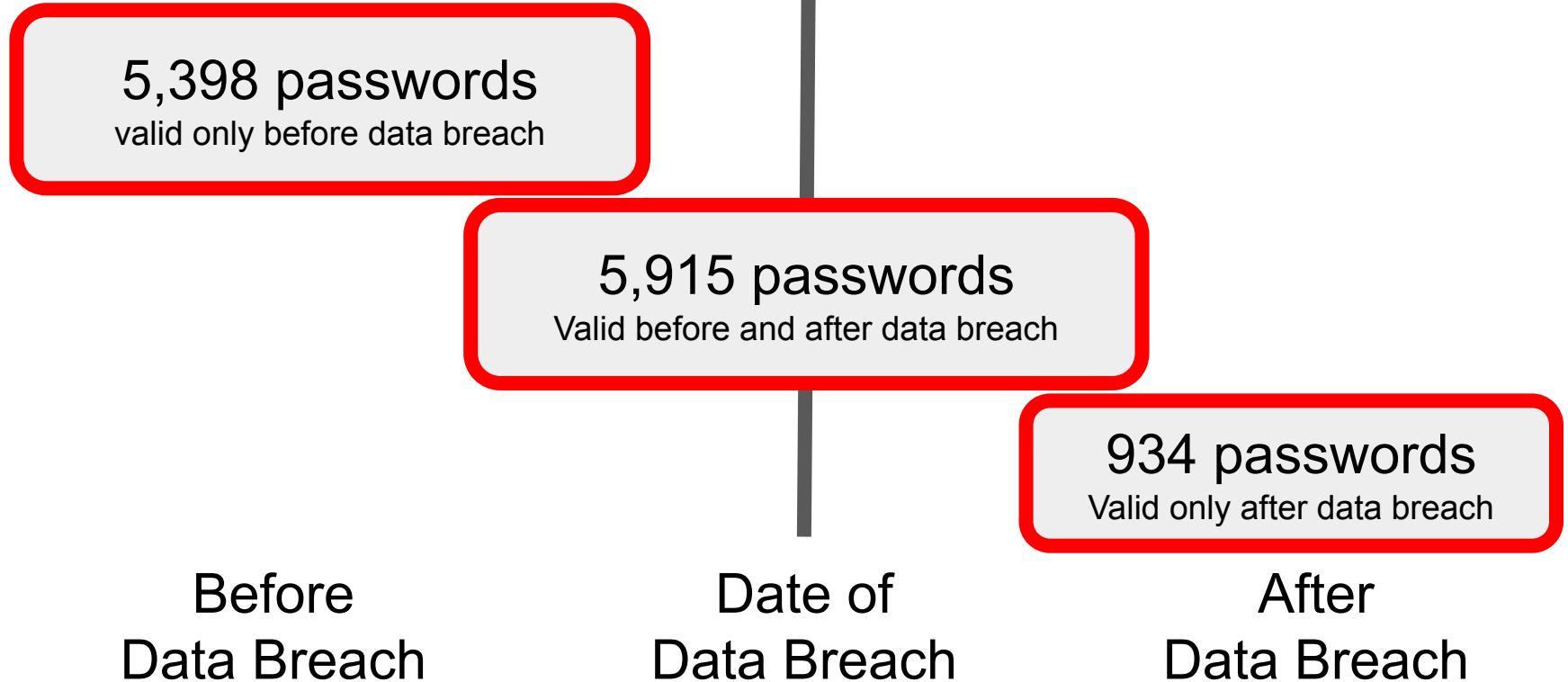
Password Reuse Is Being Exploited

Chegg





Password resets due to suspicious activity

Passwords Were Often Created at the UChicago Before They Appeared in a Data Breach



Data Breaches Impact Specific Groups of Users Differently

		
Students	11.2%	41.4%
Faculty	54.3%	2.2%

Percentages out of the number of students and faculty for which we had at least one correct guess

Plaintext
85.3%

Hashed
14.7%

Sunshine!

5F4DCC3B5AA765D61D8327DEB882CF99

correctbatteryhorsestaple

482C811DA5D5B4BC6D497FFA98491E38

i@mforg3tful!

62099D23A9D9910879D67449D9E084ED

ineedapassword

1C8F93D67A694EE1DE6363D20228DAC8

Verbatim

Reuse

54.7%

password



Password
password!
password123
p@ssw0rd
pa\$\$word

Tweaked
Passwords

45.3%

User Reactions and Experiences (n = 40)

- Users are aware they are reusing passwords
- Users know about some, but not all, relevant data breaches
- Some users were unaware they had accounts on sites that had suffered a data breach



Recommendations for Organizations



Implement processes to expire unused accounts.

;-HIBP

Using credential checking services when passwords are created isn't enough.



Promptly check high-risk (i.e., organization-related) breaches when they become public.



Check for reuse of hashed and tweaked passwords in less common data breaches.

A Two-Decade Retrospective Analysis of a University's Vulnerability to Attacks Exploiting Reused Passwords

- Password reuse was a major source of risk for UChicago
- Passwords can remain vulnerable for a long time
- Users know they are reusing their passwords, but may not know which data breaches impact them

Alexandra Nisenoff
Maximilian Golla
Miranda Wei
Juliette Hainline
Hayley Szymanek
Annika Braun
Annika Hildebrandt
Blair Christensen
David Langenberg
Blase Ur